

FIDO2 / Web Authentication

Einde der wachtwoorden?



Joost van Dijk

9 april 2019 - What's next @ SURFconext?



sa.test.surfconext.nl/registration/select-token

SURF CONEXT

Registration Portal

Authentication in two steps

English

Sign out

1. Select token

2. Link token

3. Confirm

4. Activate token

Select token



SMS



Log in with a one time SMS code. For all mobile phones.

Select



Tiqr



Log in with a smartphone app. For all smartphones with Apple iOS or Android.

Select



YubiKey



Log in with a USB hardware token. For all devices with a USB port.

Select



U2F

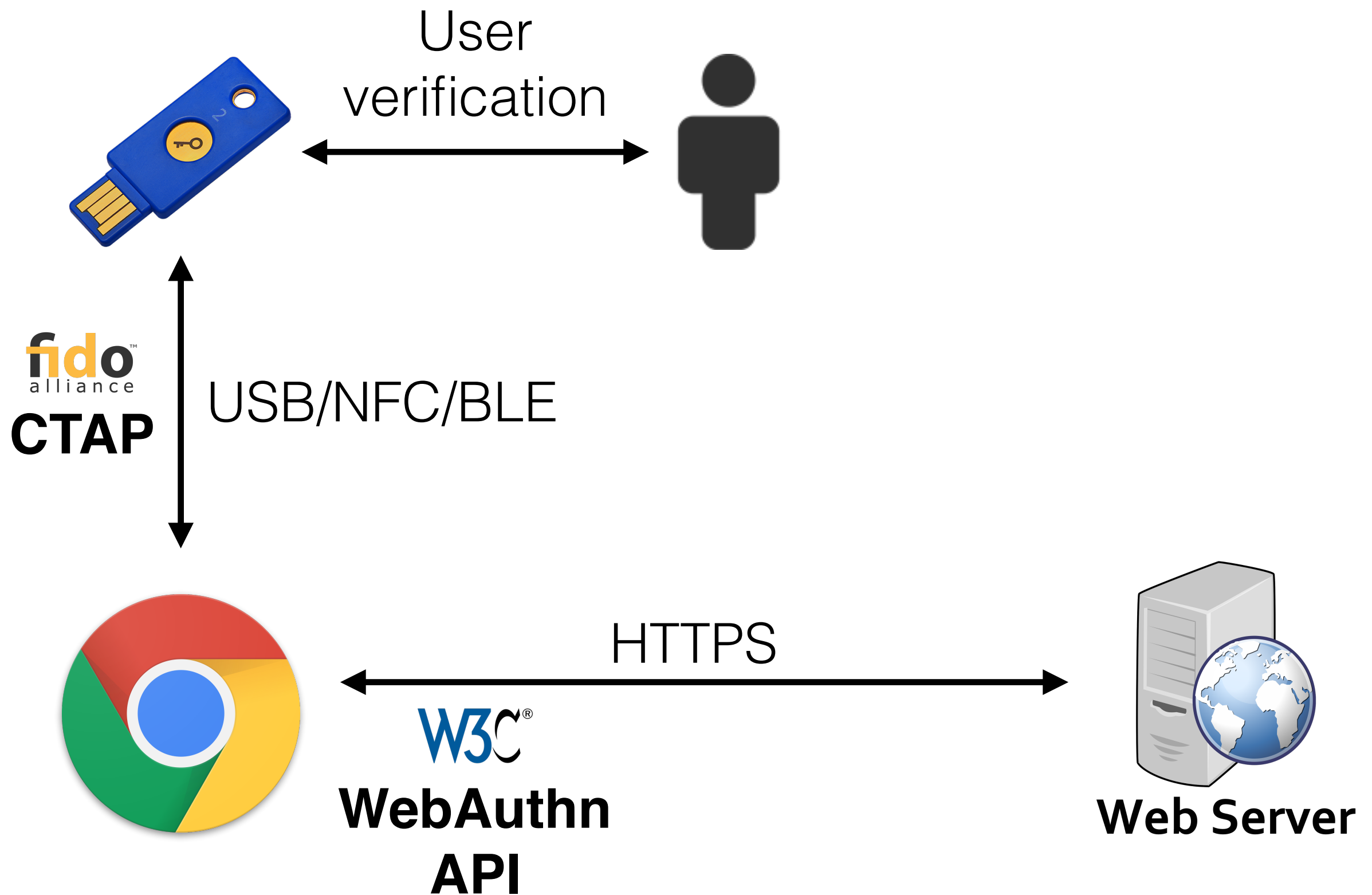


Sign in with a U2F device.

Select

Voordelen

- W3C standaard API
- Driverless
- *Device attestation*
- Public Key crypto (ECC)
- Privacy friendly (elke site een eigen key)
- *Phishing protection*
- Passwordless
- Goedkoop: hardware €10-20



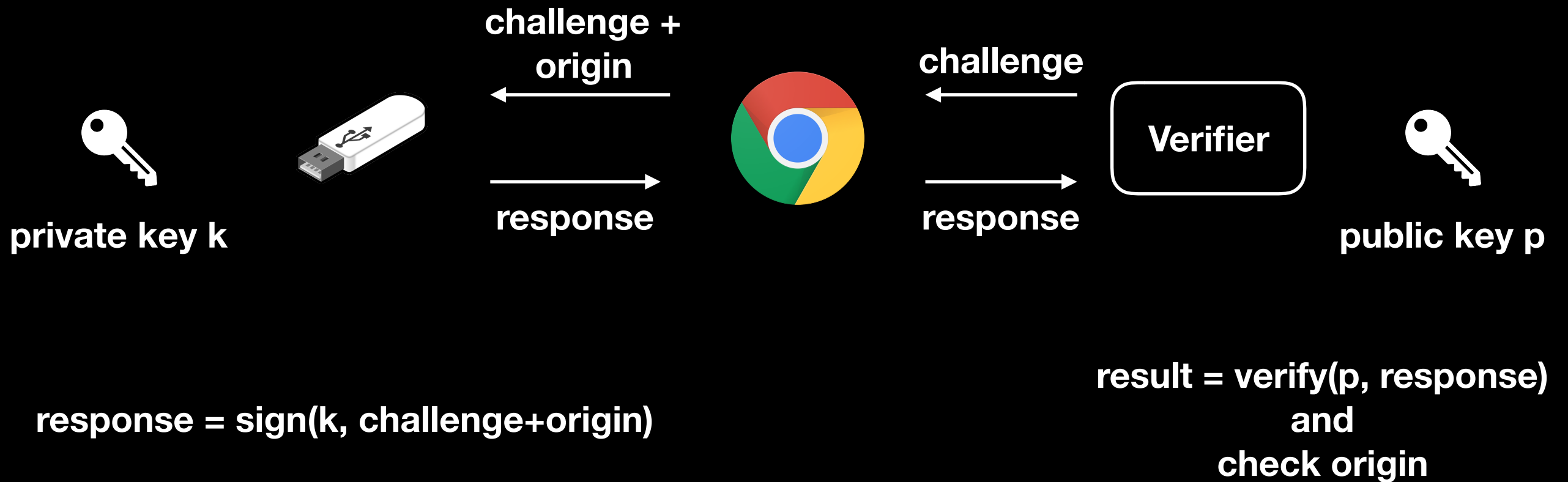
Challenge/Response authentication



Web Authentication

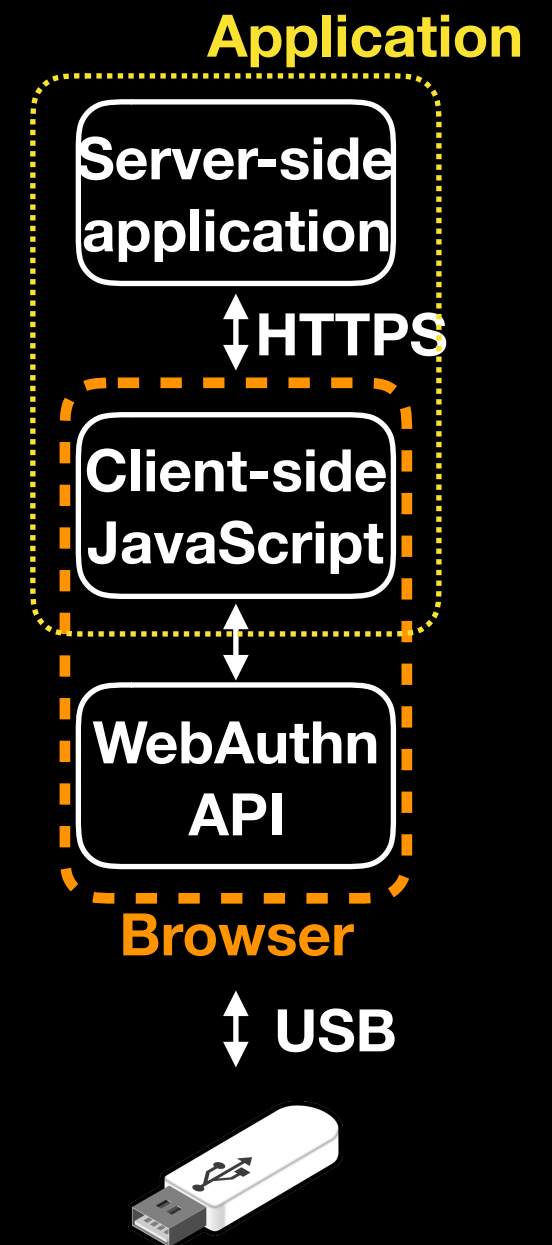


Phishing Protection



JavaScript API

- `navigator.credentials.create()`
register new key
- `navigator.credentials.get()`
authenticate using a
previously registered key



Platform Authenticator



Present your security key

Present the hardware security key that you associated with your account

Verify your identity

Confirm your fingerprint so secure.login.gov can verify it's you.



Touch sensor

Cancel

Use screen lock

Device Attestation

yk4.pem Open with Keychain Access

**Yubico U2F EE Serial
23925734811117901**

Subject Name
Common Name Yubico U2F EE Serial 23925734811117901

Issuer Name
Common Name Yubico U2F Root CA Serial 457200631

Serial Number 1013459277
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

Not Valid Before Friday, 1 August 2014 at 02:00:00 Central European Summer Time
Not Valid After Sunday, 4 September 2050 at 02:00:00 Central European Summer Time

Public Key Info
Algorithm Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key 65 bytes: 04 BD DF 67 93 DB 77 94 ...
Key Size 256 bits
Key Usage Any

Signature 256 bytes: AA C0 0D 51 09 7E EC 15 ...

Extension (1.3.6.1.4.1.41482.2)
Critical NO
Data 31 2E 33 2E 36 2E 31 2E 34 2E 31 2E 34 31 34 38 32 2E 31 2E 35

Extension (1.3.6.1.4.1.45724.2.1.1)
Critical NO
Data 03 02 05 20

Fingerprints
SHA-256 33 D4 0E 40 9F 03 57 00 F8 57 7C B9 E0 C3 7D 55 A4 07 48 2B DA AE DA
0E A3 12 29 7F BE C9 FD CF
SHA-1 2F CD 93 A0 47 F7 23 99 37 39 AF 26 EE 07 02 42 18 4A FC 2E

Browser Support

#

Web Authentication API - REC

The Web Authentication API is an extension of the Credential Management API that enables strong authentication with public key cryptography, enabling password-less authentication and / or secure second-factor authentication without SMS texts.

Usage % of all users  ?
Global 66.22%
unprefixed: 66.22%

Current aligned Usage relative Date relative Apply filters Show all ?

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Blackberry Browser	Opera Mobile *	Chrome for Android	Firefox for Android	IE Mobile	UC Browser for Android	Samsi Interr
	12	2-59	4-66		10-53										
6-10	¹ 13-17	60-64	67-71	3.1-11.1	54-57	3.2-11.4		2.1-4.4.4	7	12-12.1			10		4-7
11	18	65	72	12	58	12.1	all	67	10	46	71	64	11	11.8	8.2
		66-67	73-75	² 12.1-TP		12.2									

Notes Known issues (0) Resources (8) Feedback

WebKit status: **In Development**

¹ Can be enabled at `about:flags`

Edge 13 used an earlier draft syntax. As of Edge 14 the implementation is prefixed and based on the FIDO 2.0 Web APIs.

² Can be enabled using the Develop > Experimental Features menu. Currently supports USB-based CTAP & CTAP2 HID devices.

Questions? Remarks?



Joost.vanDijk@surfnet.nl



<http://nl.linkedin.com/in/joostd>



www.creativecommons.org/licenses/by/3.0/nl/deed.en